Strategy Research Project

Cyber Sentries: Preparing Defenders to Win in a Contested Domain

by

Lieutenant Colonel Desmond A. Reid, Jr.
United States Marine Corps

United States Army War College
Class of 2012

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
07-02-2012

2. REPORT TYPE
Strategy Research Project

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Cyber Sentries: Preparing Defenders to Win in a Contested Domain

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Desmond A. Reid, Jr.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. James E. Gordon

Department of Military Strategy,
Planning, and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Approved for public release distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Defense Department must ensure the long-term utility and security of DOD networks in the face of increasingly sophisticated state and non-state cyber threats. Developing an exceptional cyber workforce through improved training and certification programs would represent a significant step in reaching DOD security goals. This paper examines the current impediments to effective cybersecurity workforce preparation and offers new concepts to create Cyber Sentries through realistic training, network authorities tied to certification, and ethical training. These actions present an opportunity to significantly enhance workforce quality and allow the Department to operate effectively in the contested cyber domain in accordance with the vision established in its Strategy for Cyberspace Operations.

15. SUBJECT TERMS
Cybersecurity, Workforce, Cyberspace, Network Operations, Information Assurance, Certification, Credentialing, Training, Ethics

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	30	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

CYBER SENTRIES: PREPARING DEFENDERS TO WIN IN A CONTESTED DOMAIN

by

Lieutenant Colonel Desmond A. Reid, Jr.
United States Marine Corps

Dr. James E. Gordon
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Desmond A. Reid, Jr.

TITLE: Cyber Sentries: Preparing Defenders to Win in a Contested Domain

FORMAT: Strategy Research Project

DATE: 7 February 2012 WORD COUNT: 5,949 PAGES: 30

KEY TERMS: Cybersecurity, Workforce, Cyberspace, Network Operations, Information Assurance, Certification, Credentialing, Training, Ethics

CLASSIFICATION: Unclassified

The Defense Department must ensure the long-term utility and security of DOD networks in the face of increasingly sophisticated state and non-state cyber threats. Developing an exceptional cyber workforce through improved training and certification programs would represent a significant step in reaching DOD security goals. This paper examines the current impediments to effective cybersecurity workforce preparation and offers new concepts to create Cyber Sentries through realistic training, network authorities tied to certification, and ethical training. These actions present an opportunity to significantly enhance workforce quality and allow the Department to operate effectively in the contested cyber domain in accordance with the vision established in its Strategy for Cyberspace Operations.

CYBER SENTRIES: PREPARING DEFENDERS TO WIN IN A CONTESTED DOMAIN

> The development and retention of an exceptional cyber workforce is central to DoD's strategic success in cyberspace…
>
> —Department of Defense Strategy for Operating in Cyberspace

The Department of Defense (DOD) relies heavily on its cyber networks for its business, intelligence and warfighting functions. The Department currently manages 15,000 networks and seven million computing devices at all levels of security classification to exploit the advantages provided by modern technologies and networked communication.[1] With expanding network employment, a critical DOD objective must be to ensure the long-term efficacy and security of military networks in the face of increasingly sophisticated state- and non-state cyber threats. To this end, DOD will significantly enhance its cyber defense capabilities by updating the methods by which we develop the cyber workforce. This paper examines the current cybersecurity training and certification methodology to determine the impediments to effective workforce preparation and provides new concepts to improve workforce development. Ultimately, these concepts will prepare DOD "Cyber Sentries" to operate effectively in the contested cyber domain and to provide the protection required to support U. S. military freedom of action in cyberspace.

DOD continues to expand its reliance on cyber capabilities and advanced information systems for all operations. For instance, during 2010 the Department allowed its components to access commercial social media and social networking sites to exploit modern "Web 2.0" capabilities.[2] At the same time, attacks against government networks continue to rise. The U.S. Government reported a 400% increase in cyber incidents from 2006 to 2009.[3] Currently, DOD sustains millions of network probes daily, each seeking to exploit potential vulnerabilities in Department cyber networks. Additionally, advanced hacking and attack tools are increasingly capable and available to a variety of malicious cyber operators. Through successful breaches of government security systems, unauthorized personnel have retrieved "thousands of files from U.S. networks."[4] Threat actors in cyberspace include foreign intelligence services, malicious insider threats, and individuals and groups with criminal or political intent. Any of these threat actors can potentially compromise the confidentiality, integrity or availability of DOD information and systems. [5]

A high-quality cybersecurity workforce is critical to the success of security efforts designed to better protect information systems. The cybersecurity workforce, also called the information assurance (IA) workforce, includes system administrators, network operators, approving officials, privileged users and information assurance personnel. They operate and defend DOD networks, investigate anomalies, mitigate network disruptions, and implement the technical and policy controls that protect U.S. systems.[6] Highlighting their importance, the 2011 DOD Strategy for Operating in Cyberspace stated people "are the Department's first line of defense in sustaining good cyber hygiene and reducing insider threats."[7]

Unfortunately, deficiencies in the training and certification regime in use to prepare the cyberdefense workforce undermine DOD's ability to adequately address current threats. According to the Center for Strategic and International Studies, the current certification regime provides a "false sense of security," due in part to a focus on security processes which do not correlate with the technical skills required to recognize, prevent and mitigate network security intrusions.[8] Others have been unconvinced of the efficacy of certification programs, calling for operationally-focused training and performance evaluation to better serve cybersecurity personnel.[9]

Issues with the Current Methodology

Current Method Explained. Cybersecurity workforce training and certification is guided by the Information Assurance Workforce Improvement Program Manual (DOD 8570.01M, or the "Manual"). Originally signed in 2005 and updated in 2010, the Manual identifies knowledge and skill requirements for cyber network operators and defenders, detailing the qualifications necessary to perform in various cyber roles by Categories, Specialties, Levels and Functions.[10] The Manual provides a skill development baseline and process, a certification guide and the career training and experience required for military, civilian and contract personnel operating within DOD-managed cyberspace.[11]

DOD 8570.01M directs a combination of initial role-based training and on-the-job experience. For each workforce position, initial training requires some form of performance evaluation while some technical roles require an initial on-the job practical evaluation. The Manual also requires certification, appropriate to the role and experience level of the individual, within six months of assignment to a cybersecurity workforce position, with sustainment training thereafter as required by one's certification authority. All DOD personnel subject to the Manual are required to attain a commercial cybersecurity certification appropriate to their role and experience level to meet DOD 8570.01M requirements.[12] Most of these certifications require knowledge-based evaluation and many focus on applying policy directives derived from federal statutes and DOD guidance rather than applying performance-based skills.

DOD guidance requires a combination of training, certification and on-the-job experience to meet DOD 8570.01M standards. This should produce highly qualified and effective cyber network defenders. It provides a progressive training regime that requires important skills at every level to allow each individual with responsibility on DOD cyber networks to protect their cyber operations and deliver network services in support of Department missions. However, the overall quality of cyber defenders is mixed.

Current Method Outcomes. On the positive side, DOD continues to employ a vast network enterprise to accomplish its global defense mission; the overall availability of Defense Information Systems Network services, including voice, video and data communication support, is generally high. Additionally, both training compliance and workforce performance have improved in recent years according to the DOD Director of Operational Test and Evaluation (DOT&E), who is responsible for the operational evaluation of DOD networks, cyber defenses and cyber workforce quality. DOT&E evaluated 21 Service and Combatant Command exercises during Fiscal Year 2010 (FY10), including appraisals of units preparing for or already conducting combat zone deployments. The FY10 DOT&E annual report of DOD operational cyber networks indicated improved security compliance from FY05-FY10. DOT&E noted that "Experience levels and formal training levels for network defenders have increased"…and the "aggregate skill levels of network personnel assessed in several FY09 and FY10 venues indicate an increase in 'intermediate' and 'expert' skills across the Department and fewer 'beginner' level operators."[13] As a result, DOT&E

"assessments confirmed improvements in the ability to protect networks from penetration."[14]

Yet, problems persist. In Fall 2010, Deputy Secretary of Defense William Lynn admitted that DOD networks had been infected by a virus in 2008 dubbed 'agent.btz' which took 14 months to sanitize in a process labeled Operation BUCKSHOT YANKEE. Regarding this, Brookings Institution Nonresident Fellow Noah Shachtman stated, "The havoc caused by agent.btz has little to do with the worm's complexity or maliciousness — and everything to do with the military's inability to cope with even a minor threat."[15]

This anecdotal evidence is buttressed by results from official evaluations of cyber workforce performance. The Congressional Research Service reported gaps in basic cyber defender skills, stating "if systems administrators received proper training…for…keeping their computer configurations secure, then computer security would greatly improve for the U.S. critical infrastructure."[16] DOT&E agrees, asserting that despite improvements, "The ability of network defenders to detect and react to intrusions remained poor." In fact, the FY10 DOT&E annual report noted that DOT&E-sponsored adversary "Red Teams were able to overcome even the improved areas of network and systems defense during exercises," even though the cyber threat which DOT&E forces "portrayed during assessed exercises was consistently below that expected for a nation-state."[17] A DOT&E official revealed that FY11 results would maintain a similar trend.[18] In sum, improvements in training and compliance have not translated into improved performance against even low-level threat tactics.

Current Method Analyzed. The cyberdefense workforce should be markedly more capable over time not only in reducing cyber network vulnerabilities but also in detecting and responding to threats under operational network conditions. Unfortunately, a number of issues with the current training and certification regime prevent higher levels of effectiveness.

First, although cyberspace is a contested battlespace where "every networked computer is on the front line," the training and certification established under the Manual does not focus relentlessly on the adversaries that seek to illegitimately access, compromise or block DOD networks.[19] According to the Joint Operating Environment 2010 document, "cyberspace will become a main front in both irregular and traditional conflicts... Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains."[20]

Yet, cybersecurity professionals often have little understanding of the adversaries who target their systems. Current training schemes de-emphasize the enemy and the competitive nature of the cyber environment, leaving the cybersecurity workforce without the skills and understanding to succeed. Most security training and certification systems do not provide an aptitude in computer network attack techniques, though some experts contend that such training would provide defenders a much improved understanding of the threat environment.[21] Some sustainment training regimens do not require study of changing adversary tactics, tools or trends in the cyber environment. Simply put, "We have not developed our way of thinking to grasp an active defense against external threats that will both prevent penetration and neutralize threats discovered inside our networks."[22]

Second, the current methodology uses training and evaluation methods that are sub-optimal, leading to inadequate performance on DOD networks. According to a

2010 Verizon Report on government data breaches, cyber workforce errors, including poor decisions and misconfigurations are a “contributing factor in nearly all data breaches.”[23] These errors point to a need for performance-based training and testing on skills that technicians and other defenders will perform on the network in addition to their knowledge-based requirements. Although some qualifying certification programs do provide hands-on training and performance evaluation, the cyber Workforce Improvement Program does not make this mandatory or demand training in the face of an adaptive simulated threat.

Third, such errors reveal an unacceptable tolerance for performance errors despite the risks they impose. While most certification programs are rigorous and demanding, those that require knowledge-based evaluation are simply unable to examine and correct performance errors, nor can they instill an imperative to find and correct such flaws. Additionally, based on the perceived priority of network service delivery, commands sometimes accept risk in cybersecurity in favor of network service availability with unintended effects on the attitudes of cyber operators.[24] Based on these factors, defenders may not internalize their professional duty to protect DOD networks and information.

Fourth, much of current cybersecurity training is oriented toward simply hardening network defensive positions. For instance, a review of functions defined in the Manual reveals that most tasks for network and information assurance technicians, who comprise the largest block of the workforce, focus on network security policy implementation and control. None directs the collection or use of predictive intelligence regarding up-to-date adversary tactics, techniques and procedures. Few require actions to identify adverse activity within the network or the application of active countermeasures. Accordingly, many DOD 8570.01M-compliant certifications focus primarily on knowledge-based evaluations of security controls and concepts.

Unfortunately, simply hardening one's own network through the implementation of security controls and policies has proven insufficient to enable defense. Threat actors, using increasingly capable "hacking" tools are growing more sophisticated in their ability to attack networks and exploit the numerous vulnerabilities found in current network hardware, making the job of the defender ever more difficult. In fact, an expert DOD security evaluator maintained, "A well trained system administrator beats an intrusion detection device in terms of accuracy and speed."[25] Also, the speed of exploitation is increasingly outpacing the speed of defense—that is, the time it takes an attacker to identify, develop and employ an "exploit" to a previously unknown network vulnerability is generally less than the time to identify the vulnerability and then build, test and apply a "patch" to the exposure over a large network.

Therefore, even with good efforts to apply proper security protocols and practices, threat actors will likely have some success in compromising DOD networks. One senior cyber official explains, current computer network defense practice "is fundamentally reactive, not the predictive system used in the other operational domains… The approach fails in an information-age environment where software can be altered in minutes to completely change the nature of a threat."[26] Consequently, network defenders who currently focus only on building their defense lack skills to thwart, find and expel unauthorized network users.

Fifth, the significance of cybersecurity is diminished due to the low priority it receives within the overall DOD 8570.01M training framework. Cyber certification is often the last training and evaluation prerequisite for network technicians in accordance with the Manual. For example, most military network operators will receive initial technical training in formal schools where they focus on delivering network services to users. Besides providing military instruction on network operations, both the US Army and Marine Corps host technical CISCO and Microsoft Academies at their formal training centers, providing world-class training and certification to thousands of network technicians and supervisors.[27] While there is generally some security training provided in these and similar programs, the detailed security certification training required by DOD guidance can occur later, frequently decoupled from network services instruction.

This decoupling seems to reduce emphasis on cyber defense tasks. Those untrained in network operations and service delivery will generally not be granted elevated privileges on operational networks due to the potential risks posed by their lack of skill and ability. Yet, since certification is required within six months of assignment to an IA role, cyber technicians will normally have privileged network access within this period, albeit with supervision by a certified colleague. Such privileged users may be provided elevated security permissions to access system control, monitoring, administration, criminal investigation, or compliance functions on their networks.[28] In short, although the intent of the Manual is to "Provide warfighters qualified IA personnel in each category, specialty and level," the workforce improvement program allows uncertified personnel to hold important security positions for long periods.[29] This lowered “price for admission” increases the potential for mistakes and may make security seem less vital to network operators, supervisors and unit commanders.

Last, and most significant is the lack of realism in initial and sustainment training to prepare personnel for operations within the difficult and dangerous cyber battlespace. Allowing the cyber workforce to operate on “live” networks without understanding realistic attacks and associated consequences ensures both their inability to prevent threats and their propensity to approach threats without the seriousness that they deserve. However, this contradicts both joint guidance and real-world requirements. The Chairman, Joint Chiefs of Staff (CJCS) has stated “Everyone required to conduct military operations will be trained under realistic conditions and to exacting standards, prior to execution of those operations.”[30] Our cyber community is not receiving the rigorous training and evaluation that CJCS demands, to the detriment of DOD network security.

Imperatives and Options for Improvement

The Department requires a means to create a workforce of highly capable ‘Cyber Sentries’ who can better protect government networks and associated information. Analysis of the above issues reveal three imperatives for DOD workforce development modifications, including (1) increased realism in training, (2) authority in workforce roles tied to certification, and (3) a standard of professional ethics to guide the cybersecurity workforce. Significant benefit may accrue if these principles undergird changes to the cybersecurity workforce improvement program.

Increasing Realism. Training and certification programs must be made more realistic. Cyber operators must understand both the environment within which they operate and the adversary who is probing and attacking DOD networks. Joint doctrine specifies that understanding the operational environment, including relevant enemy, friendly and neutral systems, is fundamental for clear decisionmaking, effective force employment and military problem-solving.[31] To accomplish this goal, cyber operators must study and practice against adversary attack and exploitation methods. They must learn best practices to counter the adversary and rehearse how to continue effective network operations in cyberspace during significant attacks. Adversary-focused training is critical to cyber defense—it lifts the fog of uncertainty concerning threat activities and reveals adversary attributes that can be exploited for improved security. A step further in this regard would be to train advanced DOD cybersecurity professionals to operate offensively in cyberspace. Such skills would increase their knowledge of enemy techniques and procedures, and potentially offer a recruitment population for DOD's more demanding computer network attack and exploitation cadre. In either case, study of the enemy, environment and cyber attack concepts will increase realism by focusing on real-world problems and tactics and by providing a baseline of defensive performance skills to train and evaluate. The cybersecurity community must apply Sun Tzu‘s famous warfighting tenet, “Know your enemy and yourself” if they are to achieve success.[32]

Such a realistic training program requires simulation to allow the cybersecurity force to enhance and evaluate individual performance—and “allow error without consequence’’—before operating in a “live” network environment.[33] In the cyberspace domain, simulation may simply require a network disconnected from users or Internet resources. More advanced cyber training “ranges” can be developed to support instrumentation, automated adversaries or Red Team activities, simulated network subscribers and other sophisticated tools. Whether simple or complex, such an environment would allow learning through interaction with a simulated adversary and/or problem-solving against increasingly difficult cyber events.[34] In addition, competition against or cooperation with other network operators and defenders can be employed as a training method in simulated settings. Such tools and techniques can allow authentic, intense network defensive efforts and comprehensive after-action reviews to support individual and group learning, similar to the methods employed in combat arms training environments.

Several organizations sponsor cyber events using these techniques, which have even proven effective for training less experienced operators. The U. S. CyberChallenge conducts nation-wide competitions for college and high-school students to attract young Americans to the technical cybersecurity workforce. According to its Executive Director, competitions support skill development, build experience and motivation, and provide a “safe” environment to test out new cyber skills.[35] Another expert on cyber competitions explained that “passion is unlocked by competition” and when cybersecurity is seen as a type of sport, one develops a “cyber-athlete/warrior” who will dive deeper into the tradecraft of network operations and defense to gain better skills.[36] These measures allow the workforce to scrutinize enemy and friendly methods during training and learn what works.

One reason simulation, competition and other realistic training approaches are so effective is that they conform to cognitive science theories of learning. For example, one series of experiments at UCLA found that people “remember things better, longer, if they are given very challenging tests…at which they are bound to fail.”[37] Realistic simulations can provide an ideal environment for such learning. Another theory of constructivist learning postulates that students learn best within environments where they can explore and discover meaning for themselves, vice being fed information by an instructor. In this model, students are challenged to learn-by-doing; simulations can provide environments for ‘situated learning’ that focus students on the utility of acquired knowledge in real-world situations; and for ‘problem-based learning’ where students learn new information and skills by tackling complex problems.[38] Experts at the National Board of Information Security Examiners cite cognitive science developments to postulate that simulation and cyber competitions have “shown the potential…to both develop and assess cybersecurity skills” in part by providing a “working knowledge of the tactics, techniques, and procedures used by advanced or leading attackers. This knowledge helps us properly adjust security methods.”[39]

In short, the data indicate that student learning and development are best supported in realistic contexts and active learning environments.[40] Realism in practice and evaluation is effective and is an essential underpinning of a ‘Cyber Sentry’ development regime. DOD organizations are aware of many of these realities. Some DOD units are involved in cyber competitions, cyber range training and realistic venues for unit training, testing and evaluation. Such efforts support a variety of training goals for DOD cyber defenders.[41] However, these DOD activities are not required by the Manual for individual member evaluation and credentialing, undermining realism across the force.

Through the required usage of new tools and techniques, DOD can develop realistic training and evaluation for all cyber operators. Just as important, these methods must be adversary-focused to ensure network operations account for new threats and capabilities. In the end, it is the enemy, not the Manual or any certification authority, that defines the success of DOD's cybersecurity workforce. Learning how to adapt to a dynamic adversary and environment is fundamental to success. However, such training must be tied to the roles that Cyber Sentries will perform to ensure the integrity of the training regime.

Linking Authorities to Certifications. In that regard, a second imperative for change in the Manual demands that authority in network operations and defense must be coupled with a proven ability to make decisions and take actions appropriate to the threat and situation. Every cybersecurity operator must be viewed as a sentry on guard within the network—untrained sentinels are a dangerous liability. Therefore, the authority associated with elevated network administration privileges must be granted—and revoked—in accordance with proven performance throughout one's career.

Cyber network operations and security clearly constitute a vital technical field for DOD; for instance, the recently released Joint Operational Access Concept states that "Space and cyberspace are now essential …For these reasons, a joint force conducting force projection must protect its access to space and cyberspace capabilities."[42] Yet current accreditation standards seem insufficient in view of the operational requirements and threats. While certification standards are rigorous, the Manual allows up to six months of supervised operation without certification. Supervision standards and compliance mechanisms are not well defined in the DOD Directive. Notably, DOD components have not met compliance goals set by the Department for certifying their cybersecurity populations.[43] The danger is obvious; as cyber-attacks proliferate, network operators may be required to make critical decisions to defend a cyber system with little warning or preparation. Sun Tzu warns, if personnel “are unaccustomed to rigorous drilling they will be worried and hesitant in battle.”[44] One cannot expect the cyber workforce to perform at such high levels if high standards are not demanded and enforced.

Other technical fields, including healthcare, aviation, and heavy equipment operations have developed certification processes to ensure consistent training and qualification requirements for practicing members. Aviation training serves as an example. The Federal Aviation Administration (FAA) issues and requires certifications for pilots, instructors and crewmembers and specifies the conditions under which non-certified personnel may operate. The FAA also requires recent experience and proficiency checks for certified pilots and instructors under specific conditions to ensure they maintain technical currency according to expected performance standards. Both knowledge and performance evaluations are required for certification and currency. Critically, uncertified pilots are considered students who operate under strict limitations and specific supervision conditions. Certification is the threshold that demonstrates attainment of requisite knowledge, skill, aeronautical experience, and commitment to properly exercise the privilege of one’s authorizations.[45] In the aviation field, authority to perform is tied to demonstrated ability to perform, embodied in the training and credentialing system.

Aviation and cybersecurity are not directly comparable in many respects, but the technical nature of the professions and the implications of failure are similar enough to conclude that credentialing conventions similar to those in aviation would be advantageous for the cyber defense community.[46] Authority to operate should be predicated on one's demonstrated knowledge and experience to perform a specific role. Uncertified personnel should be considered students who would have strict limitations on their access to live networks until they complete the evaluation and experience prerequisites for certification. Post-certification currency standards should ensure that cybersecurity professionals renew or recertify on perishable technical skills and remain abreast of new technology and adversary techniques. This more stringent system would link privileged access and authority to training and credentials so that every Cyber Sentry is prepared to act in defense of DOD networks when required.

Developing a Standard of Professional Ethics. However, the cybersecurity workforce's ability and authority to act in defense of DOD networks must be guided by a professional ethos to ensure consistent behavior within agreed upon standards. This reveals a third imperative for workforce development: cyber operators must be well versed in the ethical requirements of the cybersecurity profession. Ethical training is common for ethical hackers who test friendly networks to identify weaknesses, while certification associations often promulgate ethical codes of conduct for their members. However, DOD lacks a comprehensive cyber ethics code and associated training to ensure cyber professionals use their important skills responsibly. Since any cyber operator could potentially take actions that are harmful or even illegal within their networks, the entire workforce warrants training to instill an 'ethic of restraint' to operate within the law and professional boundaries.

An ethic of restraint is important to prevent criminal and unethical behavior. The Department of Justice (DOJ) Internet Crime Report for 2010 identified computer crimes as among the most common internet threats.[47] Criminal use of computer network resources may include efforts to attack the computers of others; to use computers as a way to commit crimes, such as fraud; or to use computers to store illegal or stolen information, such as intellectual property.[48] Clearly, immoral end users, hackers, and criminal insiders may use legitimate or illegal access to perform illicit acts or even cause major damage within a network. However, cyber personnel with access to advanced network resources and information about users, accounts and systems can perform similar or even more detrimental activities. It is important, therefore, that all cybersecurity personnel understand unlawful and unacceptable behavior in cyberspace and be trained to act appropriately.

Beyond this, however, the DOD cybersecurity workforce requires an 'ethic of accountability', that is, a code of professional responsibility to protect DOD networks and a moral obligation to personally act in this effort. This is necessary because cyber operators, particularly those in technical roles, often cause or fail to remediate vulnerabilities in their networks. A SANS Institute whitepaper on insider threats reports "One of the main causes of monetary losses to organizations is errors and omissions accidentally and/or unknowingly made by employees, which can present an even larger problem than intentional sabotage."[49] Furthermore, employee errors, particularly those of cyber operators, can also cause loss of personal data and intellectual property, the compromise of systems or denial of network service availability. A survey of experts from the Sandia National Laboratories Information Design Assurance Red Team (IDART) program revealed that system administrators commit a variety of deliberate routine network violations, and "typically don't follow all the rules, especially with regards to firewalls" and network perimeters designed to protect computer systems.[50] In fact, the survey revealed that administrator shortcuts are generally more damaging than normal end user indiscretions, yet system administrators tend to view their own violations as unintentional or justifiable. Common violations included improper password usage, creation of "backdoors" to bypass network security systems, and failure to perform routine security-related duties. Task overload was identified as a major reason for these trends, but so was culture. Experts claimed some cyber operators thought they were exempt from network rules due to their superior security knowledge, the pressure of their roles, or their perception of security tasks as boring or a low priority.[51] In the end, these attitudes simply facilitate network vulnerabilities that can be exploited by adversaries.

DOD must instill an attitude change among cyber operators to prevent the deliberate shortcuts and unintentional errors that adversely impact Department networks. The workforce must develop a conviction to fight through attacks, deliver network capabilities and protect the Department. They must also exercise the moral courage to address task overload issues with their leaders rather than sidestep regular duties. Additionally, the cyber workforce should view data exfiltration, network compromise or unauthorized access in the same way as the loss of similar information by negligence, such as leaving a DOD facility unsecure in a high crime area. Cyber operators must accept their personal duty to protect US systems and information and must be held accountable for their actions, or lack thereof, in order to encourage professional discipline and appropriate risk management decisions. Incorporating an ethical component into the cybersecurity development regime can support these changes. The goal should be Cyber Sentries who eschew the false dichotomy of network convenience versus network security and instead seek to provide ‘secure convenience’ for all cyber operations.

DOD can realize significant improvements in network protection through incorporating three imperatives into a modified cybersecurity workforce development program. By increasing realistic knowledge, performance training venues and evaluation; by tying workforce authorities to certification and proven performance; and by instilling a professional ethos of secure convenience to guide the workforce, the Department can prepare Cyber Sentries for action in the contested cyberspace domain. Nevertheless, there are risks and concerns with any redesign of the Department’s current cybersecurity training methodology. These warrant attention to determine whether significant changes are feasible and acceptable.

Alternative Views

The training and certification upgrades identified above would be a major step toward improved performance for DOD’s cybersecurity workforce. However, some argue that certifications may not be worth the cost, time, or resources.[52] An analyst from the Information Technology and Innovation Foundation estimates it may cost nearly $40 million to certify the federal cyber workforce and an additional $6 million annually to maintain these certifications based on current DOD 8570.01M standards.[53] Expanding certification requirements through additional training, testing or new certifications may further escalate these costs. Moreover, increased training time and higher standards may disqualify many within the current workforce and reduce DOD’s pool of available cyber personnel and recruits. Also, while a National Cyber Range facility presently exists that may provide a virtual environment to meet some of the proposed stipulations, it is possible that even more training venues and resources will be necessary.

These are significant concerns. Nevertheless, these may be mitigated in several instances. The population requiring the proposed certifications would remain roughly the same as that presently mandated by the Manual. As with existing standards, the current cyber workforce must be provided an opportunity to meet the new guidelines once implemented in policy. However, for both new accessions and current cyber personnel, better training should result in a high certification success rate to maintain a sufficient population. Improved training realism, techniques and technology may better facilitate learning and moderate training duration. Also, while it is true that additional training resources may be necessary, many existing network venues and low cost tools may be utilized to support enhanced training, thereby limiting some costs. Additional rigor in training, testing and certification as proposed above will likely lead to a more favorable cost-benefit analysis, particularly in view of the continued cost of attacks against DOD networks.

Another concern is that independent DOD action to change its certification, training and authority policies may have adverse impacts on the Interagency and commercial entities. For example, other federal agencies require interoperability with DOD networks and therefore may be affected by DOD workforce modifications. Additionally, since both industry certification groups and the cybersecurity industry are heavily invested in DOD cybersecurity, impacts to these partners and their constituents must also be considered. As well, Congress has considered the issue of strengthening cyber workforce requirements for over two years; the Senate has introduced draft legislation regarding cybersecurity and internet freedom.[54] DOD efforts must consider Legislative actions at the outset to synchronize with Congressional intent.

It is true that DOD would need to coordinate any changes closely with industry, the Interagency and Congress to prioritize security program modifications and to secure resources to support the new program. Yet this presents an opportunity to collaborate on standards for cyber roles, training and other requirements with both government and civilian partners. The improvements proposed would enhance the importance of the certification industry, which would likely generate a more operationally relevant credentialing process for all government agencies. On the contrary, inaction may fail to capitalize on political and industry support for improvements that should significantly enhance security.

Some might suggest workforce quality improvement simply by directing a low-cost apprenticeship program and more performance testing requirements in DOD 8570.01M. Such a plan would have to be more stringent than current regulations but could theoretically benefit the Department without incurring significant costs or changes to the Manual. Yet, fiscal obligations are already projected to rise to meet existing Manual requirements with uncertain effects on workforce competency.[55] Opportunities for apprenticeship exist today, but suffer from the current lack of supervision standards, lack of training realism and insufficient certified “masters” to teach novices and journeymen. And, without a specific focus on the adversary, operators may still have difficulty transitioning from training to the network environment. In short, any security gains would be difficult to quantify against the additional resources and effort required.

Overall, while there are a number of potential concerns with upgrading the current cyber training and certification regime, the above examination demonstrates that the most significant issues can either be mitigated or discounted. Alternative concepts also fall short of satisfying the training needs of the cyber community.

Recommendation

Clearly, the cybersecurity workforce development process warrants upgrades. To realize the goal of creating Cyber Sentries, the Department must take concrete steps to implement change. DOD must amend DOD 8570.01M to require simulation and other realistic training activities; deny access to privileged user status until certification is complete; and incorporate an ethics requirement in training programs. These actions will update the Manual to meet the CJCS directive for realistic training prior to entering into military operations. To implement this guidance, knowledge, skill, ability and ethical standards must be developed for each cyber role to ensure that the new requirements are incorporated appropriately within the career development pipeline.[56] Toward this end, the US National Institute for Science and Technology draft cybersecurity workforce framework, which standardizes roles with associated tasks and skills, can serve as an outline for DOD efforts.[57] The Manual will also need to delineate authorities associated with each role and certification, as well as "currency" requirements to ensure training remains up-to-date.

Beyond these actions, the Department will also need to develop several supporting products. A DOD cyber ethics code is necessary to guide actions across the workforce. Simulation tools, cyber challenges, cyber ranges and other capabilities must be distributed appropriately to support DOD training efforts. Synchronization with the intelligence community will be important to enable a constant focus on the adversary and the dynamic cyber environment. Training systems and standards are needed to support currency requirements. Authority should be extended to Inspector General and Operational Test and Evaluation organizations to monitor compliance and support standards. Most important, all DOD actions must be coordinated with government and industry partners to ensure success at each step. Only then can the Department obtain and synchronize the support framework necessary to implement this new concept.

Conclusion

The President has categorized cybersecurity as a critical national security issue and has identified the digital workforce as a critical aspect of reducing risk in cyberspace.[58] DOD has developed a cyberspace operating strategy that includes the "development and retention of an exceptional cyber workforce."[59] Success in developing such quality would allow the Department to exploit the talent and ingenuity of our human capital toward generating a competitive advantage in cyberspace operations. DOD could then also serve as an example and assistant to partners in industry, academia and foreign governments. However, failure to improve the workforce may signal a lack of resolve to the American public, our partners, and our adversaries. Most important, without progress in workforce development, the Department simply may not be able to counter the increasingly capable malicious attacks against DOD network infrastructure.

The Defense Department must ensure the long-term utility and security of DOD networks in the face of increasingly sophisticated state- and non-state cyber threats by developing an exceptional cyber workforce. This paper examined the current impediments to effective cybersecurity workforce preparation and offered new concepts to create Cyber Sentries through realistic training, network authorities tied to certification, and ethical training. These actions present an opportunity to significantly enhance workforce quality and allow the Department to operate effectively in the contested cyber domain in accordance with the vision established in its Strategy for Cyberspace Operations.

Endnotes

[1] Department of Defense, *DOD Strategy for Operating in Cyberspace*, (Washington, DC: Department of Defense, July 2011), 1.

[2] U. S. Deputy Secretary of Defense William J. Lynn III, "Directive-Type Memorandum (DTM) 09-026 - Responsible and Effective Use of Internet-based Capabilities", memorandum for Secretaries of the Military Departments, et al, Washington DC, February 25, 2010.

[3]Gregory C. Wilshusen, *CyberSecurity: Continued Attention Is Needed to Protect Federal Information Systems from* Evolving *Threats*, Testimony presented to the Committee on Homeland Security, House of Representatives (Washington, DC: U.S. Government Accountability Office, 2010), 3-4.

[4] Department of Defense, *DOD Strategy for Operating in Cyberspace*, (Washington, DC: Department of Defense, July 2011), 3.

[5] DoD defines the terms confidentiality (assurance that information is not disclosed to unauthorized individuals, processes, or devices), integrity (protection against unauthorized modification or destruction of information), and availability (timely, reliable access to data and information services for authorized users). See Committee on National Security Systems, *National Information Assurance Glossary*, CNSS Instruction No. 4009 (Ft Meade MD: Secretariat (I42) National Security Agency, May 2003), 5, 15, 34.

[6] John G. Grimes, "Information Assurance Workforce Improvement Program," (Washington DC, Department of Defense, Incorporating change 2 as of April 20, 2010), 85-86.

[7] Department of Defense, *DOD Strategy for Operating in Cyberspace*, (Washington, DC: Department of Defense, July 2011), 7.

[8] Karen Evans and Frank Reeder, *A Human Capital Crisis in Cybersecurity, Technical* Proficiency *Matters: A Report of the CSIS Commission on Cybersecurity for the 44th President*, (Washington D.C.: Center for Strategic and International Studies, November 2010) , 3-4.

[9] Daniel Castro, "The Role of Professional Certification in Securing Information Systems," October 14, 2009, http://itif.org/publications/role-professional-certification-securing-information-systems (accessed November 13, 2011), 1-2.

[10] Definitions for each are as follows: Categories. The DoD IA workforce is split into two major categories of Technical and Management. IA manager refers to personnel performing any IA management function. Levels. Each of the IA workforce categories has three levels (Technical or Management Level 1, 2, and 3). The management category also includes the DAA position. Functions. The specific IA job requirements associated with a category and level. The functions provide a means to distinguish between different levels of work. The functional level indicates the roles that an employee performs or occupational requirements to successfully perform at different levels of the IA Workforce. The functional level approach also encourages a broader, more integrated means of identifying what an employee must know to perform the tasks that comprise an IA position across all of the DoD Components. Deputy Secretary of Defense, “Information Assurance Training, Certification, and Workforce Management,” (Washington DC, Department of Defense, current as of April 23, 2007), 8; and John G. Grimes, “Information Assurance Workforce Improvement Program," (Washington DC, Department of Defense, Incorporating change 2 as of April 20, 2010), 82.

[11] John G. Grimes, “Information Assurance Workforce Improvement Program," (Washington DC, Department of Defense, Incorporating change 2 as of April 20, 2010), 11.

[12] John G. Grimes, “Information Assurance Workforce Improvement Program," (Washington DC, Department of Defense, Incorporating change 2 as of April 20, 2010), 20-41, 60-80.

[13] J. Michael Gilmore, *DOT&E FY2010 Annual Report,* (Washington DC: Director, Operational Test and Evaluation, December, 2010), 258.

[14] J. Michael Gilmore, *DOT&E FY2010 Annual Report,* (Washington DC: Director, Operational Test and Evaluation, December, 2010), 258-259.

[15]Noah Shachtman, “Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack,” August 25, 2010, http://www.brookings.edu/opinions/2010/0825_pentagon_worm_shachtman.aspx (accessed November 28, 2011).

[16] Clay Wilson, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress* (Washington, DC: U.S. Library of Congress, Congressional Research Service, October 17, 2003), 6.

[17] J. Michael Gilmore, *DOT&E FY2010 Annual Report,* (Washington DC: Director, Operational Test and Evaluation, December 2010), 257-259.

[18] Mr. David Aland, Technical Director IA/Interoperability Assessment Program, Office of the Director, Operational Test and Evaluation, Office of the Secretary of Defense, telephone interview by author, January 4, 2012.

[19] U. S. Joint Forces Command, Joint Operating Environment, JOE 2010 (Suffolk, VA: U. S. Joint Forces Command Joint Futures Group (J59), February 18, 2010), 36.

[20] U. S. Joint Forces Command, *Joint Operating Environment*, JOE 2010 (Suffolk, VA: U. S. Joint Forces Command Joint Futures Group (J59), February 18, 2010), 36.

[21] Ms. Renee McGlaughlin, Executive Director, U.S. Cyber Challenge, Center for Internet Security, telephone interview by author, October 31, 2011; Dr. Daniel Manson, Professor, Computer Information Systems, California State Polytechnic University, Pomona, telephone interview by author, December 9, 2011; Mr. Matthew Mayes, Former National Security Agency Red Team Leader, interview by author, November 6, 2011.

[22] Rear Admiral William E. Leigher, "Learning to Operate in Cyberspace," US Naval Institute Proceedings, February 2011, 33.

[23] Verizon Security Solutions White Paper, "Cybersecurity: Protecting Our Federal Government From Cyber Attacks," 2010, http://www.verizonbusiness.com/resources/whitepapers/wp_protecting-us-federal-government-from-cyber-attacks_en_xg.pdf (accessed 22 December 2011), 2.

[24] CAPT Jill Newton, U.S. Navy, National Security Agency, interview by author, Ft Meade, MD, October 27, 2011.

[25] Mr. David Aland, Technical Director IA/Interoperability Assessment Program, Office of the Director, Operational Test and Evaluation, Office of the Secretary of Defense, telephone interview by author, January 4, 2012.

[26] Rear Admiral William E. Leigher, "Learning to Operate in Cyberspace," US Naval Institute Proceedings, February 2011, 33.

[27] CISCO Networking Academy, "Impact at U.S. Federal Government Agencies," 2011, http://www.cisco.com/web/learning/netacad/us-can/docs/Federal-Profile-2011.pdf (accessed December 3, 2011).

[28] Deputy Secretary of Defense, "Information Assurance Training, Certification, and Workforce Management," (Washington DC, Department of Defense, current as of April 23, 2007), 9.

[29] John G. Grimes, "Information Assurance Workforce Improvement Program," (Washington DC, Department of Defense, Incorporating change 2 as of April 20, 2010), 11.

[30] Chairman Joint Chief of Staff, *The Joint Training System: A Primer for Senior Leaders*, CJCS Guide 3501 (Washington, DC: Joint Staff J7, Current as of July 7, 2010), 9.

[31] U. S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, DC: U. S. Joint Chiefs of Staff, August 11, 2011), IV-1 to IV-3.

[32] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 84.

[33] Orson Scott Card, *Ender's Game*, (New York: Tor Books, 1991), xiv.

[34] Michael J. Assante and David H. Tobey, "Enhancing the Cybersecurity Workforce," *IT Professional* 13, no. 1 (January-February 2011): 15.

[35] Ms. Renee McGlaughlin, Executive Director, U.S. Cyber Challenge, Center for Internet Security, telephone interview by author, October 31, 2011.

[36] Dr. Daniel Manson, Professor, Computer Information Systems, California State Polytechnic University, Pomona, telephone interview by author, December 9, 2011

[37] Henry L. Roediger and Bridgid Finn, " Getting It Wrong: Surprising Tips on How to Learn" *Scientific American*, October 20, 2009, http://www.scientificamerican.com/article.cfm?id=getting-it-wrong (accessed December 2011).

[38] U. S. Marine Corps, *Systems Approach to Training Manual*, (Quantico, VA: Marine Corps Training and Education Command, June 4, 2004), 6-20 to 6-23.

[39] Michael J. Assante and David H. Tobey, "Enhancing the Cybersecurity Workforce," *IT Professional* 13, no. 1 (January-February 2011): 13-14.

[40] John D. Bransford, Ann L. Brown, and Rodney R. Cocking, *eds.* with additional material from the Committee on Learning Research and Educational Practice and the Commission on Behavioral and Social Sciences and Education National Research Council, *How People Learn: Brain, Mind, Experience, and School: Expanded Edition*, (Washington, DC: National Academy Press, 2000) 235-243.

[41] Robert Powell, Timothy K. Holmes, and Cesar E. Pie, "The Information Assurance Range," *ITEA Journal* 31, no. 4 (December 2010): 473–477.

[42] Martin E. Dempsey, *Joint Operational Access Concept* version 1.0 (Washington, DC: U. S. Joint Chiefs of Staff, January 17, 2012), 26-27. http://www.defense.gov/pubs/pdfs/JOAC_Jan%202012_Signed.pdf (accessed February 1, 2012).

[43] Mr. George Bieber, "Certification in DoD," briefing slides from Office of the Assistant Secretary of Defense Networks and Information Integration, March 17, 2011, http://csrc.nist.gov/organizations/fissea/2011-conference/presentations/March17_FISSEA-Certifications-GBieber.pdf (accessed February 6, 2012).

[44] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 66.

[45] Title 14 Code of Federal Regulations, "Aeronautics and Space, Part 61 Certification: Pilots, Flight Instructors, And Ground Instructors," http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=40760189a03dfea0b501608f33820a45&rgn=div5&view=text&node=14:2.0.1.1.2&idno=14#PartTop (accessed December 14, 11), Subpart A 61.1-61.5, 61.17, 61.56-58, Subpart C 61.89, Subpart G 61.193.

[46] Michael J. Assante and David H. Tobey, "Enhancing the Cybersecurity Workforce," *IT Professional* 13, no. 1 (January-February 2011): 13-14.

[47] Internet Crime Complaint Center , *2010 Internet Crime Report* (Washington, DC: National White Collar Crime Center and U. S. Department of Justice) 10, 19. http://www.ic3.gov/ media/annualreport/2010_ic3report.pdf (accessed February 1, 2012).

[48] The Cybercitizen Awareness Program "What is cybercrime?" Webpage http://cybercitizenship.org/crime/crime.html (accessed December 17, 2011).

[49] Dr. Eric Cole, "Correlating SIM information to Detect Insider Threats," June 2007, linked from SANS Home Page at "Reading Room," http://www.sans.org/reading_room/ analysts_program/SIMInfo_June07.pdf (accessed February 1, 2012), 6.

[50] S. Kraemer, P. Carayon, and J. F. Clem, "Characterizing violations in Computer and Information Security Systems,"2006, linked from University of Wisconsin - Madison Center for Quality and Productivity Improvement Human Factors in Computer and Information Security Publications at "Papers," http://cqpi.engr.wisc.edu/system/files/IEA.pdf (accessed February 1, 2012), 2.

[51] S. Kraemer, P. Carayon, and J. F. Clem, "Characterizing violations in Computer and Information Security Systems,"2006, linked from University of Wisconsin - Madison Center for Quality and Productivity Improvement Human Factors in Computer and Information Security Publications at "Papers," http://cqpi.engr.wisc.edu/system/files/IEA.pdf (accessed February 1, 2012), 2; 4-6.

[52] Daniel Castro, "The Role of Professional Certification in Securing Information Systems," October 14, 2009, http://itif.org/publications/role-professional-certification-securing-information-systems (accessed November 13, 2011), 1-2.

[53] Daniel Castro, "The Role of Professional Certification in Securing Information Systems," October 14, 2009, http://itif.org/publications/role-professional-certification-securing-information-systems (accessed November 13, 2011), 2.

[54] "Cybersecurity Act of 2009," (Introduced April 1, 2009), S.773.IS, http://www.opencongress.org/bill/111-s773/show (accessed 11 November 2011); and "Cybersecurity and Internet Freedom Act of 2011" (Introduced in Senate) S.413.IS http://www.gpo.gov/fdsys/pkg/BILLS-112s413is/pdf/BILLS-112s413is.pdf (accessed November 11, 2011).

[55] Daniel Castro, "The Role of Professional Certification in Securing Information Systems," October 14, 2009, http://itif.org/publications/role-professional-certification-securing-information-systems (accessed November 13, 2011), 1-2.

[56] U. S. Marine Corps, *Systems Approach to Training Manual*, (Quantico, VA: Marine Corps Training and Education Command, June 4, 2004), 6-20 to 6-23; and CAPT Jill Newton, U.S. Navy, National Security Agency, interview by author, Ft Meade, MD, October 27, 2011.

[57] National Institute of Standards and Technology, *National Initiative for Cybersecurity Education-Cybersecurity-Workforce Framework* (National Institute of Standards and Technology, September 2011); and linked from National Initiative for Cybersecurity Education-

Cybersecurity-Workforce Framework Page http://csrc.nist.gov/nice/framework/documents/NICE-Cybersecurity-Workforce-Framework-printable.pdf (accessed December 22, 2011).

[58] Barack Obama, National Security Strategy (Washington, DC: The White House, May 2010), 27-28.

[59] Department of Defense, DOD Strategy for Operating in Cyberspace, (Washington, DC: Department of Defense, July 2011), 10-11.